ECS Configuration Change Request

Page 1 of Page(s)

1. Originator Henry Baez	**2. Log Date:** **4/10/03**	**3. CCR #:** **03-0257**	**4. Rev:**	**5. Tel:** 301-925-1025	**6. Rm #:** 2101D	**7. Dept.** Sys Eng

8. CCR Title: Install PORTUS smwrap.5061 and message file patch on DAACs and SMC firewalls.

9. Originator Signature/Date **Henry Baez, /s/ 4/10/03**	**10. Class** **II**	**11. Type:** **CCR**	**12. Need Date:** 04-16-2003

13. Office Manager Signature/Date **Carolyn Whitaker /s/ 4/10/03**	**14. Category of Change:** Initial ECS Baseline Doc.	**15. Priority: (**If "Emergency" fill in Block 27). Routine
16. Documentation/Drawings Impacted *(Review and submit checklist):*	**17. Schedule Impact:**	**18. CI(s) Affected:**
19. Release Affected by this Change: 6A	**20. Date due to Custome r:**	**21. Estimated Cost:** None - Under 100K

22. Source Reference: □**NCR (attach)** □**Action Item** □**Tech Ref.** □**GSFC** □**Other:**

23. Problem: (use additional Sheets if necessary)
There is a new vulnerability in sendmail. This vulnerability is based on mis-treatment of the ASCII character 255 in e-mail addresses in message headers. This vulnerability is based on the message headers, and thus can be passed to internal sendmail servers, not just the one on the firewall.

24. Proposed Solution: (use additional sheets if necessary)
Install Portus new version of smwrap and message patch which will convert the char (255) to char (127) before passing the message on to sendmail. IBM will also release a new sendmail client but for now replacing the sendmail proxy, smwrap, will provide the protection needed against this type of attack. This fix is for version of Portus 5.05. Need to have this install first. The tar file is called smwrap_5061.tar, size is 204800, sum values are 58529 400

25. Alternate Solution: (use additional sheets if necessary)
None.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)
Failing to install this version of smwrap will put at risk security of internal sendmail servers.

27. Justification for Emergency (If Block 15 is "Emergency"):

28. Site(s) Affected: □EDF □PVC □VATC ☒EDC ☒ GSFC ☒LaRC ☒NSIDC ☒SMC □AK □JPL
□EOC □ IDG Test Cell □Other

29. Board Comments:	**30. Work Assigned To:**	**31. CCR Closed Date:**

32. EDF/SCDV CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
33. M&O CCB Chair (Sign/Date): **Gary Gavigan /s/ 04/15/03**	**Disposition:** [✓ Approved] App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
34. ECS CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ESDIS

ADDITIONAL SHEET

CCR #: **Rev:** **Originator:** Henry Baez

Telephone: 301-925-1025 **Office:** 2101D

Title of Change: Install PORTUS smwrap.5061 and message file patch on DAACs and SMC firewalls. .

Prerequisites - The firewall has to be running PORTUS software version 5.05.

Installation Instructions - The upgrade takes less than a minute. There will be minimal disruption to email traffic.
1. Login as root on firewall.
2. Crate a directory under /tmp called smwrapfix2 and cd to it.

```
#mkdir /tmp/smwrapfix <Enter>
#cd /tmp/smwrapfix2 <Enter>
```

3. FTP the smwrap_5061.tar to the firewall directory /tmp/smwrapfix2.
4. With the command 'tar xvf smwrap_5061.tar extract the files.

```
#tar –xvf smwrap_54061 <Enter>
```

5. Check the file size and sum values a follows:

File Name	Size	Sum
smwrap.506_1	119970	60275 118
portus.cat.506_1	80160	58961 79

Note: If the checksum is NOT correct, stop and contact Landover for new tar file or other way to get correct files.

6. Check that the owner, group and permissions on the files match the following.

```
#ls –l /tmp/smwrapfix2 <Enter>
-r--r--r--   1 root    system    80160 Mar 31 12:54 portus.cat.506_1
-r-xr-xr-x   1 root    system   119970 Mar 31 15:19 smwrap.506_1
```

Replace smwrap and portus.cat with new Binaries Installation
1. Now save the present version of the smwrap and portus.cat file in the directory /usr/local/etc/ as follows:

```
#cd /usr/local/etc <Enter>
#cp smwrap smwrap.[date of change] <Enter>
#cp portus.cat portus.cat.[date of change] <Enter>
```

2. Change back to the /tmp/smwrap2 directory
3. Copy the files from /tmp/smwrapfix2 to /usr/local/etc as follows:

```
#cp portus.cat.506_1 /usr/local/etc/portus.cat <Enter>
#cp smwrap.506_1 /usr/local/etc/smwrap <Enter>
```

These final commands will replace your existing smwrap program and message catalog with the new versions. Smwrap is run by the fwcop (the PORTUS firewall inetd like program) only when an email comes in. There might be a second or two where an email might not be processed during the copy.

Note: You do not have to shutdown and rebooted the firewall.

Verification of Installation

Check that email is flowing by checking for first smwrap entries in the syslog file as follows:

```
#tail -f /var/ad/syslog | grep smwrap <Enter>
```

After seeing smwrap entire, you can check for sendmail entries if configured for them in syslog:

```
#tail -f /var/ad/syslog | grep sendmail <Enter>
```

Due to the number of entries in the firewall syslog, some sites do not have sendmail recording enable on the firewall syslog.

The smwrap file is different then the smwrapd daemon that you would see if you do a ps -ef.

Back-Out Instructions

The older version of portus.cat and smwrap can just be copied back from the portus.cat.[date of change] and smwrap.[date of change] in the /usr/local/etc directory.